Open Science Enclave (OSE)
Baseline Security Configuration

Prepared by: _____ Date: _____
FermiGrid Project Leader
Keith Chadwick

Approved by: _____ Date: _____
Computer Security Executive Officer
Victoria White

Document Revision History:

Version	Date	Author	Comments
0.0	31-Aug-07	Keith Chadwick	Initial draft version.
0.1	01-Jan-08	Keith Chadwick	Document after1st Review and Modifications by OSE Working Group

Table of Contents

1.0 INTRODUCTION

This Security Technical Implementation Guide (STIG) provides Fermi National Accelerator Laboratory with guidance regarding the proper configuration of computing resources (i.e. systems) in the Fermilab Open Science Enclave (OSE) in accordance with the Fermi National Accelerator Laboratory security requirements and guidelines. This document will focus on Scientific Linux and the Open Science Grid (OSG) Middleware (typically the Virtual Data Toolkit) as used in the Fermilab Open Science Enclave environment.

The Fermi National Accelerator Laboratory Security Baseline configuration settings represent industry best practices for securing Grid computing resources, based on recommendations from several sources, including the Open Science Grid collaboration, the Virtual Data Toolkit, and the Fermilab Open Science Enclave Working Group (OSEWG). These settings were reviewed and modified for compliance with the Fermi National Accelerator Laboratory operational environment.

This document presents the minimum (mandatory) and recommended (best practice) levels of security settings.

1.1 Purpose

The settings discussed in the STIG are intended to minimize the exposure of computing resources in the Fermilab Open Science Enclave to known vulnerabilities, and to reduce the risk of compromise of computing resources in the General Computing Enclave.

1.2 Scope

This document presents the minimum (mandatory) and recommended (best practice) configurations of all computing resources within the Fermilab Open Science Enclave. A computing resource is administratively defined as being in the Fermilab Open Science Enclave if it meets the following definition:

Open Science Enclave Computing Resource Definition:

A computing resource must be part of the Open Science Enclave (OSE) if it is managed by Fermilab and allows grid users to install and/or run software using credentials which are not issued and revocable by Fermilab.

Other explicitly identified computing resources supporting the operation of the OSE may be designated part of the OSE by Fermilab.

1.3 Key Word Interpretations

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119:

http://www.ietf.org/rfc/rfc2119.txt

1.4 Intended Audience

This document is intended for system and service administrators responsible for the security of computing resources within the Fermilab Open Science Enclave. It assumes that the reader has knowledge of the Scientific Linux operating system, Grid Middleware, and is familiar with common computer technology and common administrative tasks.

2.0 PHYSICAL SECURITY

Production Grid computing resources in the Fermilab Open Science Enclave must be physically secured to ensure that unauthorized individuals do not gain access to the systems. Placing the computing resource in a managed computer floor with keycard-controlled access is recommended.

2.1 System BIOS Password

Setting the firmware password is not mandatory for computing resources in the Fermilab Open Science Enclave.

2.2 Authentication for Single User Mode

All computing resources in the Fermilab Open Science Enclave should be configured to require authentication to enter single user mode.

2.3 Console Logout

The console (physical display head and/or serial port) must be logged out when an authorized system or service administrator is not actively managing a computing resource in the Fermilab Open Science Enclave.

3.0 REGISTRATION, LOGIN BANNER, DOE STICKERS AND INVENTORY

All computing resources in the Fermilab Open Science Enclave must be appropriately registered in the following databases:

- The computing resource MAC address(es) must be registered with MISCOMP/MISNET.

- The computing resource node name(s) must be registered with MISCOMP/EQIUPDB.

- The System Administrators of the computing resource(s) must be registered with MISCOMP/SysadminDB.

All computing resources in the Fermilab Open Science Enclave must display the Fermilab "Policy on Computing" DOE Banner on the Interactive Login Screen or Login Service, and must also display the corresponding DOE sticker on the physical display head.

All computing resources in the Fermilab Open Science Enclave must participate in the Fermilab central systems management and inventory services and the Fermilab Open Science Enclave management and inventory services. No computing resource may explicitly prohibit or deny access from the FNAL computer security scanning.

4.0 SECURE INSTALLATION

Prior to placing a Grid computing resource into production the system administrator must ensure that the latest patches were installed. Specifically:

- Any operating system patches declared "critical" or "mandatory" must be installed before connecting to the Fermilab network.

- Any Grid middleware patches declared "critical" or "mandatory" must be installed before Grid access is enabled.

Unnecessary or unused services are to be disabled. Access controls must be implemented wherever possible to limit the exposure of the computing resource to both local and remote users, using the least privilege access methodology.

It is recommended to start with a "clean" install from known good media, particularly if the prior configuration of the computing resource is not well known (i.e. you "inherit" an old system, you are not sure what is on it, best practice is to wipe the system and install clean).

4.1 Supported Operating System

All computing resources in the Fermilab Open Science Enclave must have a "supported" operating system (typically a supported version of Scientific Linux or Scientific Linux Fermi with optional Xen kernel modifications).

4.2 Automatic Daily Updates

All computing resources in the Fermilab Open Science Enclave must participate in the Fermilab central patching services (e.g. for Scientific Linux, the default yum.cron should be in /etc/cron.daily/).

All computing resources in the Fermilab Open Science Enclave must maintain an up-to-date list of valid Certificate Authorities (CAs) and corresponding Certificate Revocation Lists (CRLs). The CRLs must be maintained with a maximum "refresh" interval of 24 hours (1 day).

>>> Need to figure out how to notify (whom?) when the CRL is older than 31 days.

4.3 Patch Management

All computing resources in the Fermilab Open Science Enclave must install all "critical" or "mandatory" patches (OS and Grid Middleware) within one week of the patch release or sooner if directed by the Fermilab Computer Security Coordinator.

4.4 Anti Virus

Not currently applicable.

4.5 Personal Identifiable Information

In compliance with the Fermilab policy on Personal Identifiable Information, all computing resources in the Fermilab Open Science Enclave are forbidden from collecting, displaying or retaining Protected Personal Identifiable Information.

5.0 ACCOUNT POLICIES

The following account policies apply to all computing resources in the Fermilab Open Science Enclave:

5.1 Empty password entries are not allowed.

Empty password fields are not allowed in the password file.

5.2 UID 0 on root entry only

The UID of "0" (zero) must be assigned to the root user only.

5.3 Local account password policy

The local password policy must adhere to the Fermilab Strong Authentication Policy.

For local accounts, their passwords must adhere to the following three conditions:

- The password hash must be stored locally (no NIS, LDAP, etc.), and should be stored in a shadow password file which is not world readable.
- The password cannot be used for network access (restrict to securetty).
- The password cannot contain the user's Kerberos password and cannot be similar to it.

5.4 Use of Administrator or root Accounts

The use of administrator (root) accounts should be minimized.

5.5 Grid Service Accounts

Grid services should be configured to execute with the least necessary privileges. Any account used by a Grid service must be a valid UID/GID combination that was previously registered in the CD UID/GID database.

5.6 Interactive User Accounts

All compute resources in the Fermilab Open Science Enclave must be configured to follow the Fermilab Strong Authentication policy for all "interactive" or "user" login accounts.

The number of authorized general user login accounts and access should be minimized. The following guidelines should be taken into account:

- Less than 5 to 10 percent of total accounts for an experiment?
- Process for an experiment requesting and/or granting interactive access?
- List of reasons why interactive access is granted (special roles)?
- List of accounts that have interactive access must be maintained?

All unused accounts in the password file should be blocked.

All user accounts must be a valid UID/GID combination that was previously registered in the CD UID/GID database.

5.7 Grid Accounts

Accounts which are used to execute Grid jobs must be configured with a login shell of /sbin/nologin.

Production compute resources in the Fermilab Open Science Enclave must be configured to obtain and implement the DN+FQAN to USERNAME mapping from the FermiGrid GUMS Server (gums.fnal.gov / fermigrid3.fnal.gov).

The compute resource in the Fermilab Open Science Enclave is responsible for mapping the USERNAME returned by GUMS to a valid UID/GID combination that was previously registered in the CD UID/GID database.

Production compute resources in the Fermilab Open Science Enclave must be configured to obtain and implement the Site AuthoriZation decisions from the FermiGrid SAZ Server (saz.fnal.gov / fermigrid4.fnal.gov).

5.8 Pilot Jobs

Within the Fermilab Open Science Enclave, Pilot jobs are defined as follows:

Pilot Job Definition:

A multi-user pilot job, hereafter referred to simply as a pilot job, is a Grid job owned by one member of a Virtual Organization (VO) which during execution at a Site pulls down and executes workload, hereafter called a user job, owned and submitted by a different member of the VO or multiple user jobs owned and submitted by multiple members of the VO.

All compute resources in the Fermilab Open Science Enclave that accept "pilot jobs" must have the gLExec product installed and configured.

<insert additional gLExec configuration wordsmithing here from Igor and Keith>

Pilot jobs are allowed only if a formal trust relationship exists between the VO and Fermilab that explicitly authorizes the use of pilot jobs. The VO shall provide Fermilab information on how to distinguish pilots authorized by the VOs from other jobs (eg. the VO must identify the DN and/or Roles that shall be authorized to execute pilot jobs at Fermilab).

Fermilab shall maintain a list of VOs possessing such a trust relationship together with the list of authorized DNs and Roles.

6.0 NETWORKING AND NETWORK SERVICES

The following network and network service policies apply to all computing resources in the Fermilab Open Science Enclave.

6.1 Turn Off Unneeded Services

Any services that are not essential to the computing resource operation should be disabled (turned off).

6.2 Bridging and Routing

Compute resources in the Fermilab Open Science Enclave are not allowed to offer network bridging and routing services, unless they are hosting Virtual Machines (VMs) (typically Xen or VMware):

- If the compute resource is hosting one or more virtual machines, then the **"host"** or **"domain 0"** system (hypervisor) may be configured to offer network bridging and/or routing services to the **internal** virtual machines running on that individual **"host"** or **"domain 0"** system.

- The compute resource may not be configured to offer bridging or routing services to external resources.

6.3 Firewalls

Any services that are essential to the computing resource operation should be examined for appropriate firewall rules (typically via iptables or ipchains). Where possible, the firewall configuration should restrict connections to services to the minimal set of systems and/or services necessary for operation.

In particular, if the computing resource is participating in the FermiGrid jobmanager-cemon based job forwarding, and is accepting "limited proxies", then the iptables firewall on the computing resource should be configured to restrict connections to the Globus Gatekeeper ports (2119 and 9443) as strictly as possible, but in any case to allow none from outside the Fermilab subnet (131.225.x.x).

6.4 Login Services

All "interactive" or "user" login services shall be configured to follow the Fermilab Strong Authentication policy.

All production "grid" job submission services shall be configured to use GSI (certificate) based authentication. The GSI authorization shall be configured to use the FermiGrid Site Authorization service (saz.fnal.gov / fermigrid4.fnal.gov) and the FermiGrid Grid User Mapping Service (gums.fnal.gov / fermigrid3.fnal.gov).

6.5 Service Authentication

Services on compute resources in the Fermilab Open Science Enclave should be configured to securely authenticate (Kerberos and/or GSI) with the corresponding client.

6.6 WWW, Web Server and Web Services

Compute resources in the Fermilab Open Science Enclave may be configured to offer World Wide Web (WWW) services. Where the web services are intended for access without authentication, refer to the Apache baseline configuration. Where the web services are intended for GSI based access, the compute resource web services should be configured as recommended by the Open Science Grid collaboration together with the recommendations from the Virtual Data Toolkit software distributions:

https://twiki.grid.iu.edu/twiki/bin/view/Documentation/WebHome
http://osg-docdb.opensciencegrid.org/
http://vdt.cs.wisc.edu//index.html

6.7 Database

Compute resources in the Fermilab Open Science Enclave may offer unauthenticated database query (read) access. Compute resources that intend to offer database write or update access must be secured according to the corresponding database baseline(s). Access to the database should be restricted to localhost.

6.8 NIS

NIS services are allowed.

6.9 NFS

Compute resources in the Fermilab Open Science Enclave (OSE) must not be configured as NFS file servers to the General Computing Enclave (GCE).

NFS clients are allowed. The recommended NFS server is the Fermilab Computing Division managed "BlueArc" NFS Server Appliance.

Note that significant restrictions may be required on either the file system NFS server or NFS client depending on the relative enclave locations of the NFS server and the NFS client. These restrictions are detailed in the "File Systems and Directories" section of the OSE Baseline.

6.10 AFS

Compute resources in the Fermilab Open Science Enclave are not authorized to provide AFS file services. Compute resources in the Fermilab Open Science Enclave may be configured as AFS clients.

Note that significant restrictions may be required on either the file system AFS server or AFS client depending on the relative enclave locations of the AFS server and the AFS

client. These restrictions are detailed in the "File Systems and Directories" section of the OSE Baseline.

6.11 Other File Services

Compute resources in the Fermilab Open Science Enclave are not authorized to provide other network based file services (such as SMB, CIFS or AFP), or to be configured as the corresponding client.

6.12 LDAP

Compute resources in the Fermilab Open Science Enclave must not be configured to offer LDAP services for authentication.

6.13 SMTP

Compute resources in the Fermilab Open Science Enclave are not authorized to provide email services (including SMTP, POP and IMAP) on the network. Compute resources in the Fermilab Open Science Enclave may be configured to allow outbound mail in accordance with Fermilab email policies:

http://computing.fnal.gov/email/

6.14 SNMP

Compute resources in the Fermilab Open Science Enclave must not allow SNMP write operations on the Fermilab public network.

6.15 IPMI

Compute resources in the Fermilab Open Science Enclave that offer or have IPMI services must have those services connected to a dedicated private network.

6.16 TFTP

Compute resources in the Fermilab Open Science Enclave must not be configured as TFTP servers across the Fermilab public network backbone.

6.17 DNS and DHCP

Compute resources in the Fermilab Open Science Enclave are not authorized to provide DNS services.

Compute resources in the Fermilab Open Science Enclave are not authorized to provide DHCP services, unless they are hosting Virtual Machines (VMs) (typically Xen or VMware):

- If the compute resource is hosting one or more virtual machines, then the **"host"** or **"domain 0"** system (hypervisor) may be configured to offer DHCP services to the **internal** virtual machines running on that individual **"host"** or **"domain 0"** system.

- The compute resource may not be configured to offer DHCP services to external resources (over the network).

6.18 XDMCP and X Services

Compute resources in the Fermilab Open Science Enclave are not allowed to offer XDMCP services.

X service on a system in the Fermilab Open Science Enclave with a display head is allowed, but the X server must not be configured to accept network connections.

6.19 Boot Services

Compute resources in the Fermilab Open Science Enclave should not be configured as boot servers.

6.20 Modem (Dial-in) and Wireless Services

Compute resources in the Fermilab Open Science Enclave must not be configured to offer modem (dial-in) or wireless access point equivalent services.

7.0 GRID MIDDLEWARE AND GRID SERVICES

All compute resources in the Fermilab Open Science Enclave must adhere to the following Grid Middleware and Grid Service requirements.

7.1 Sources for selected Grid Middleware Components

All production compute resources in the Fermilab Open Science Enclave must have those components of "base" Grid middleware installed from the official OSG or EGEE grid middleware repositories or authorized mirrors:

Grid	Grid middleware repository name	Grid middleware repository URL
OSG	VDT	http://vdt.cs.wisc.edu//index.html
EGEE	gLite	http://glite.web.cern.ch/glite/default.asp

The “base” Grid middleware is defined as those components that provide job authentication, authorization, execution and file transfer:

http://vdt.cs.wisc.edu//index.html

The version of the “base” Grid middleware that is installed on the compute resource must be a version that has current support from the corresponding Grid middleware repository.

Note: When installing multiple simultaneous copies of the Grid middleware, the installation should be configured to use the FermiGrid Squid server (squid.fnal.gov:3128) as a http_proxy server in order to minimize the impact of the installation on offsite file servers and reduce the likelihood of the offsite file server accesses triggering the network autoblocker.

7.2 Modifications to the Grid middleware

Any modifications to Grid middleware following the initial installation must be carefully performed to insure that:

- Any required or necessary bug fixes are not prevented, disabled or removed.
- All security mechanisms and controls remain in place.

7.3 Certificate Authorities

Any additions to the set of Certificate Authorities, other than routine installations of updated CA-Certificates packages that are distributed by the Grid middleware repository, must be approved by the Fermilab Computer Security Coordinator.

7.4 Configuration of files and directories in /etc/grid-security

All computing resources in the Fermilab Open Science Enclave are recommended to make the directory /etc/grid-security/certificates a symlink to:

$GLOBUS_LOCATION/TRUSTED_CA

The host certificate and host keys must be stored in /etc/grid-security with the permissions specified below:

File	Required Permissions
hostcert.pem	644
hostkey.pem	600

It is recommended that a backup of these files be maintained offline.

7.5 Globus Gatekeeper

All production compute resources in the Fermilab Open Science Enclave must have their Globus gatekeepers configured to use GUMS and SAZ through the gsi-authz.conf, prima-authz.conf and sazc.conf files located in the /etc/grid-security directory.

Note: The Site AuthoriZation (SAZ) service should be invoked prior to the Grid User Mapping Service (GUMS). This configuration reduces the load on the GUMS server, since if a Grid credential fails authorization by the SAZ server, the Globus gatekeeper does not invoke the GUMS service.

7.6 GridFTP

Production compute resources in the Fermilab Open Science Enclave that offer public GridFTP services must be configured to obtain and implement the DN+FQAN to USERNAME mapping from the FermiGrid GUMS Server (gums.fnal.gov / fermigrid3.fnal.gov).

The compute resource in the Fermilab Open Science Enclave is responsible for mapping the USERNAME returned by GUMS to a valid UID/GID combination that was previously registered in the CD UID/GID database.

Production compute resources in the Fermilab Open Science Enclave that offer public GridFTP services should be configured to obtain and implement the Site AuthoriZation decisions from the FermiGrid SAZ Server (saz.fnal.gov / fermigrid4.fnal.gov).

Note: If the compute resource is both a Globus Gatekeeper and a GridFTP server, the use of SAZ is mandatory.

7.7 Virtual Organization Member Registration Service (VOMRS)

Compute resources in the Fermilab Open Science Enclave may not offer public VOMRS services unless they are authorized to do so by the Fermilab Computer Security Coordinator.

7.8 Virtual Organization Management Service (VOMS)

Compute resources in the Fermilab Open Science Enclave may not offer public VOMS services unless they are authorized to do so by the Fermilab Computer Security Coordinator.

7.9 Grid User Mapping Service (GUMS)

Compute resources in the Fermilab Open Science Enclave may not offer public GUMS services unless they are authorized to do so by the Fermilab Computer Security Coordinator.

7.10 Site AuthoriZation Service (SAZ)

Compute resources in the Fermilab Open Science Enclave may not offer public SAZ services unless they are authorized to do so by the Fermilab Computer Security Coordinator.

7.11 Web Servers (including Apache and Tomcat)

All compute resources in the Fermilab Open Science Enclave should disable indexing by placing the following robots.txt file in the web server document root directories:

robots.txt

```
User-agent: *
Disallow: /
```

The typical apache and tomcat document root directories are:

- $VDT_LOCATION/apache/htdocs
- $VDT_LOCATION/tomcat/v5/webapps
- $VDT_LOCATION/tomcat/v5/webapps/tomcat-docs

7.12 Worker Node (gLExec)

Production compute resources in the Fermilab Open Science Enclave that have the gLExec product installed must be configured to obtain and implement the DN+FQAN to USERNAME mapping from the FermiGrid GUMS Server (gums.fnal.gov).

The compute resource in the Fermilab Open Science Enclave is responsible for mapping the USERNAME returned by GUMS to a valid UID/GID combination that was previously registered in the CD UID/GID database.

Production compute resources in the Fermilab Open Science Enclave must be configured to obtain and implement the Site AuthoriZation decisions from the FermiGrid SAZ Server (currently fermigrid4.fnal.gov, soon to be saz.fnal.gov).

7.13 Squid Web Cache

All compute resources in the Fermilab Open Science Enclave are recommended to be configured to use the FermiGrid Squid server (squid.fnal.gov:3128) as an http proxy server.

In the event that an organization elects to instantiate their own Squid server(s), the experiment is responsible for assuring the compliance of their Squid server(s) with the requirements of Fermilab computer security policies.

7.14 MyProxy

Compute resources in the Fermilab Open Science Enclave must not offer MyProxy services on the network unless they are authorized to do so by the Fermilab Computer Security Coordinator.

All MyProxy services at Fermilab must be configured to require X.509 certificate authentication to store and retrieve proxies. MyProxy services must not be configured to allow passphrase authentication to store and retrieve proxies.

7.15 VOBox or Edge Services

Compute resources in the Fermilab Open Science Enclave may not offer VOBox or Edge Services unless they are authorized to do so by the Fermilab Computer Security Coordinator.

Questions for a Xen baseline discussion:

- How are versions of the virtual machine "snapshots" of images tracked?
- How are moves, adds and changes administered?
- How are virtual machine and application dependencies kept in check?
- How are user and administrative roles managed across virtual machines?
- What forensics are available to help determine why a virtual machine when down?

Keith – do we need to create a Xen baseline???

8.0 FILE SYSTEMS & DIRECTORY REQUIREMENTS

All compute resources in the Fermilab Open Science Enclave must adhere to the following file system and directory requirements.

8.1 NFS File Systems

Compute resources in the Fermilab Open Science Enclave should be configured with the following NFS file system permissions:

- User home areas of General Computing Enclave computer accounts are not to be made accessible in the Open Science Enclave. Requests for read-only Open Science Enclave access may be considered but if granted, would be subject to additional controls to be determined.

- All shared file systems writable in the Open Science Enclave must have the "noexec" option set wherever they are mounted in the General Computing Enclave. This includes the file server itself if it is in the General Computing Enclave.

8.2 AFS File Systems

The presence of AFS tokens in the OSE should be minimized, and in particular reasonable steps should be taken to minimize the possibilities of token sharing or stealing in the presence of shared accounts.

This may be accomplished through the use of:

- AFS access without tokens.

- GUMS pool accounts (permanent 1-1 DN to UID mapping), coupled with token destruction on job exit.

- Group accounts that are used by multiple DNs require PAGs (Process Authorization Groups) [Note there are problems with PAGs in the 2.6+ Kernel]…

8.3 Certificates and Certificate Storage

All system, host or service credentials should be stored in /etc/grid-security with 444 permissions on the public certificate and 400 permissions on the private key (or equivalent ACL based permissions). All private keys should be readable only by root and the UID that the service starts under.

Individual user credentials (private key) must not be stored in such a way that exposes them to other unprivileged users on the system or network. Users should note that storage of credentials on NFS or AFS served volumes is fraught with significant risks. User credentials (private keys) that are valid for more that 1x10E6 seconds, must be protected with a suitably strong passphrase. Individuals should store a backup of their credentials in a location subject to the access requirements stated above.

Use of DOEgrids service certificates to run automated workflows is subject to the requirement of an explicit formal trust relationship between the user offering the service and the administrator of the system on which the service is running.

8.4 Umask for non-root

The umask setting that controls access by user, group and other, must disallow write by other for non-root users (002), and wherever possible should disallow all access by group and other (077).

8.5 Umask for root

The umask setting for root must disallow write by group and other (022), and wherever possible should disallow all access by group and other (077).

8.6 Home Areas

Home areas and “dot files” must not be writable by other.

8.7 777 Directories

It is recommended that all world writeable directories have the “sticky” bit set.

9.0 LOGGING

Compute resources in the Fermilab Open Science Enclave must be configured to log system and grid middleware service logs.

Logs should be stored locally and forwarded to the central Fermilab log servers via syslog-ng.

9.1 System Log Retention and Rotation

System logs should be rotated daily (or more often if necessary). The use of logrotate is encouraged.

At least 31 days of system logs must be maintained online, and all system logs must be backed up and available via a backup restore for a minimum of 1 year.

9.2 Grid Middleware Logs

Grid middleware service logs should be rotated daily (or more often if necessary). The use of logrotate is encouraged.

Service	Log and Typical Location
Globus Gatekeeper (Pre Web Services)	$GLOBUS_LOCATION/var/globus-gatekeeper.log
Globus Gatekeeper (Web Services)	$GLOBUS_LOCATION/var/container-real.log
VOMS	$VDT_LOCATION/glite/log/voms.*vo-name* $VDT_LOCATION/tomcat/v5/voms-admin.*vo-name*.log
VOMRS	$VDT_LOCATION/tomcat/v5/vomrs-*vo-name*.log
GUMS	$VDT_LOCATION/tomcat/v5/gums-service-admin.log
SAZ	$VDT_LOCATION/saz/server/sazserver.log
Squid	/etc/syslog
MyProxy	/etc/syslog

At least 31 days of Grid middleware service logs must be maintained online, and all Grid middleware service logs must be backed up and available via a backup restore for a minimum of 1 year.

9.3 Syslog-Ng and Splunk

Compute resources in the Fermilab Open Science Enclave are encouraged to use syslog-ng, and furthermore syslog-ng should be configured to send a copy of the log files to the central Fermilab Splunk service.

9.4 File Permissions on log files

Log files on compute resources in the Fermilab Open Science Enclave should be configured with a minimum of 644 permissions, with 640 or 600 permissions preferred.

10.0 ACCOUNTING

All compute resources in the Fermilab Open Science Enclave must be configured to report to the appropriate Gratia accounting repository.

11.0 BACKUP & RECOVERY

Backups of the computing resource are the responsibility of the data owner. Support of the computing resource is the responsibility of the computing resource owner.

12.0 REFERENCES

Fermilab Common Unix Class Baseline Security Configuration
Fermilab Scientific Linux Fermi 3.0.x and 4.x Baseline Security Configuration
Fermilab Computer Security Plan
Fermilab Open Science Enclave Security Plan
FermiGrid Authentication Infrastructure Minor Application Security Plan

Appendix 1 - List of Currently Authorized Restricted Services

Service	Who	Where	Comments
VOMRS	FermiGrid	fermigrid2	
		fgtest2	
VOMS	FermiGrid	fermigrid2	
		fg5x1	
		fg6x1	
		fgtest2	
GUMS	FermiGrid	fermigrid3	
		fg5x2	
		fg6x2	
		fgtest3	
		fgtest5	
SAZ	FermiGrid	fermigrid4	
		fg5x3	
		fg6x3	
		fgtest4	
		fgtest6	
MyProxy	FermiGrid	fermigrid4	
Edge Services	FermiGrid	fermigrid0	

Appendix 2 – NFS Permission Matrices

Maximum Allowed Permissions:

Served from / Exported to		"Home" and "System" File Systems	
		GCE	OSE
Compute Resource	GCE	**full access (rwx)**	**no access**
	OSE	**no access**	**full access (rwx)**

Maximum Allowed Permissions:

Served from / Exported to		"Data" and "Project" File Systems	
		GCE	OSE
Compute Resource	GCE	**full access (rwx)**	**read, write, noexec (rw-)**
	OSE	**read, nowrite, exec (r-x)**	**full access (rwx)**

Appendix 3 – OSE Compliance Summary – 01-Jan-2008

System/Cluster	Experiment / Stakeholder	Compliant to Baseline	Comments
fermigrid1-6	FermiGrid	Yes	
fgtest1-6	FermiGrid	Yes	
fngp-osg	Multiple small experiments	No	Users have login access to OSE systems, file systems shared across GCE and OSE
fgitb-gk	FermiGrid & OSG	Yes	
gpmpi	Multiple small experiments	Yes	
fcdfosg1	CDF	Yes	
fcdfosg2	CDF	Yes	
fcdfosg3	CDF	Yes	
fcdfosg4	CDF	Yes	
d0cabosg1	D0	No	Users have login access to OSE systems, file systems shared across GCE and OSE. gLexec deployment.
d0cabosg2	D0	No	Users have login access to OSE systems, file systems shared across GCE and OSE. gLexec deployment.
cmsosgce	CMS	No	Has not deployed SAZ gLexec deployment
cmsosgce2	CMS	No	Has not deployed SAZ gLexec deployment
cmsosgce3	CMS	No	Has not deployed SAZ gLexec deployment
cmsosgce4	CMS	No	Has not deployed SAZ gLexec deployment

Appendix 4 – OSE Compliance Detail Matrix – 01-Jan-2008